

Enterprise Identity Management 101

Phillip J. Windley
Brigham Young University
phil@windley.com
www.windley.com

Digital Identity Matters



Rifkin on service economy and what it portends for identity: commercial transactions based on property can be relatively anonymous, not services. This raises the burden of authentication

Trends:

Service economy

Reduced anonymity

Electronic delivery

Result:

Digital identity matters!

What is an Identity?



An **Identity** is a set of:

Attributes - medical history, past purchasing behavior, bank balance

Preferences - currency used, what brand of hot dog you like, blue background on the screen

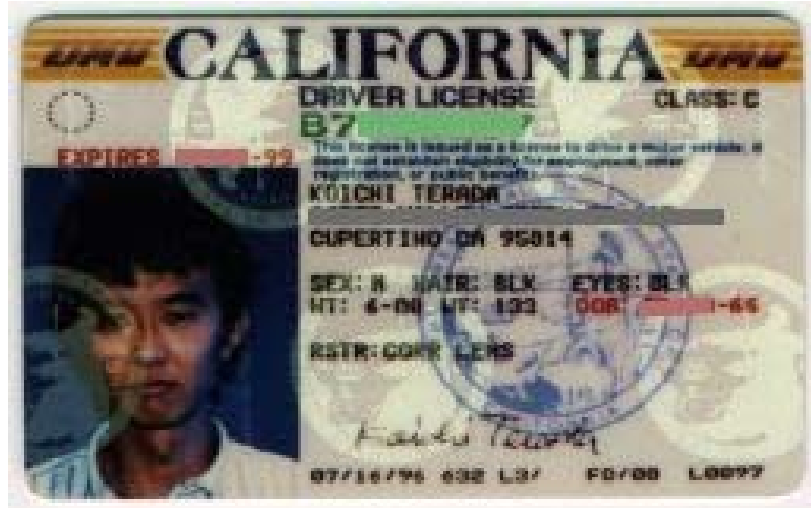
Traits - eye color, where a business was incorporated

About a **subject**

Subjects make requests relative to a **resource**

Outside looking in or inside looking out. Inside looking out is more holistic. Concentrate on that, even if you're outside. It drives user behavior and attitudes.

Credentials



Evidence of the right to an identity

Transfer of trust

Policy enforcement point (**PEP**) **authenticates** credentials

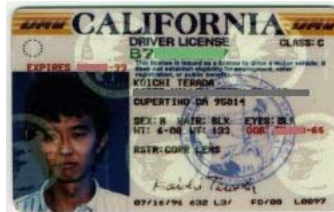
Policy decision point (**PDP**)

determines **permissions** and **entitlements**

In accordance with an **access policy**

PDP communicates a **authorization decision assertion** to the PEP

Buying Beer



Driver's license

Identity

Attributes

Preferences

Traits

Authentication

Authorization

Credit card

Signed credential

External PDP

When a person (i.e. the subject) wants to buy beer (i.e. perform an action on a resource), the clerk (i.e. security authority) examines the license to see if it looks real (i.e. determines the validity of the credential) and uses the picture (i.e. embedded biometric device) to see if the person presenting the license is the same person who owns it (i.e. authenticates the credential). Once certain that the license is authentic, the clerk, reads the birth date (i.e. attribute) from the license and determines whether the person is over 21 (i.e. consults a security policy determined by the state and makes a policy decision about permissions associated with the identity).

The credit card (a separate identity/credential) is presented to the

What Happened to the Walls?



www.windley.com

6

City defenses were based on walls.

Limits commerce

Trebuchet made city walls obsolete

The Border Patrol



Corporate security is likewise based on a perimeter strategy.

Limits commercial activity, but has been driven by IT based on a security analysis.

Recent trends reduce this strategy to rubble. Examples:

VPNs and Wi-Fi

Web Services

Business Context of Identity



VS



Traditionally focused on machines and networks

Business needs will drive security policies

Policies need to talk about

- Documents

- Actions

- Data

- People

Security has been focused on defense

Digital identity is focused on opportunity:

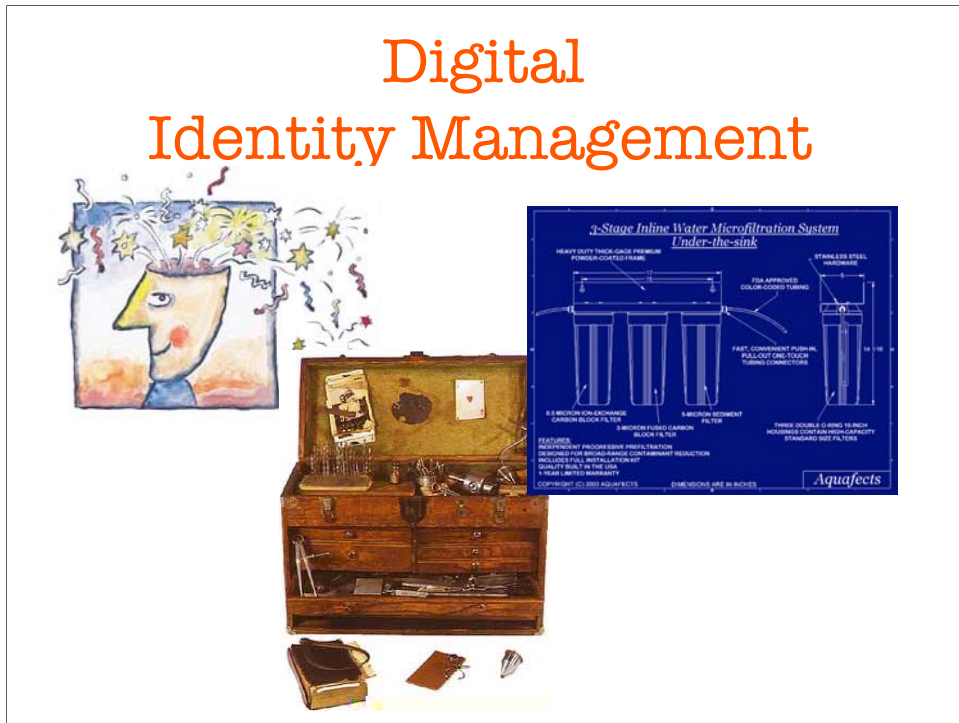
- Employees

- Partners

- Customers

Properly implemented digital ID strategy is an enabler for other strategic initiatives

Digital Identity Management



Concepts, tools, ways to plan

How to manage:

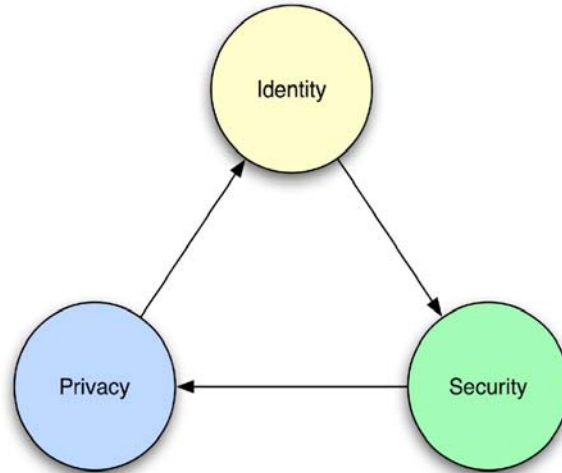
Thousands of resources

Thousands of subjects

Hundreds of systems

Fine-grained access control

Security, Trust, & Privacy



Identity Federation



SourceID

PingIdentity
CORPORATION

WS-Federation
WS-Federation

- Linking identities across organizations
- Sharing attributes and authentication
- Loose coupling
- Goes beyond technology standards
 - Policy
 - Liability
 - Governance
 - Trust

Single sign-on between organizations

Goes beyond technology standards

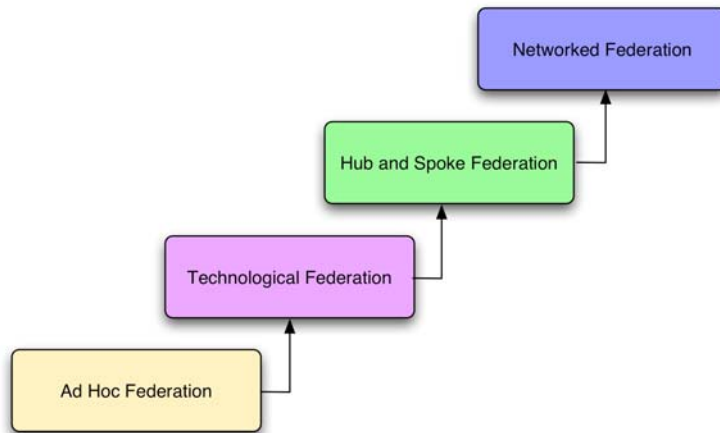
Policy

Politics

Governance

Legal issues

Federation Maturity



Story of iMall and Verio: ad hoc

Hub and spoke federation driven by large central players in a market

Story of Bank of America, BankAmericard, Visa

Accountability vs. Enforcement



“Accountability
is a log
processing
problem”

-Dan Geer

- Access control scales geometrically (its a table)
- Accountability scales linearly
- Access control systems are incredibly vulnerable to DDoS attacks

Controlling access to everything is very hard. Maybe impossible.

Digital Rights Management



www.windley.com

14

Digital leakage

DRM is about controlling access beyond the corporate border.

Controlling data or controlling customers?

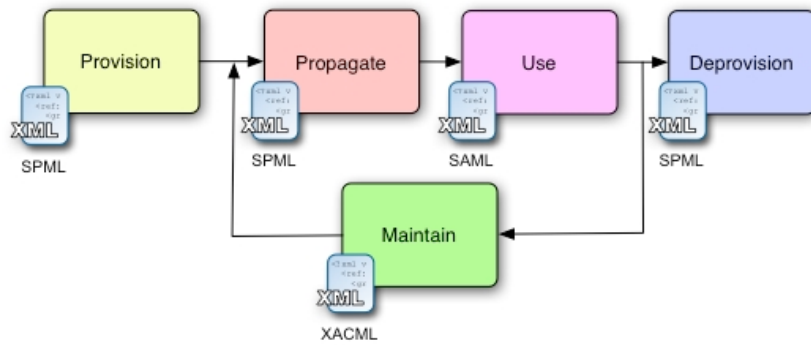
Restricting rights costs money.

Apple iTunes as a cautionary tale

- Balance rights with price
- Heavy administrative burden
- Upset customers

Trusted computing

Open Identity Standards



Provides scaffolding for building identity systems

Starts simple and builds in complexity

- Integrity & Non-repudiation: *XML Signature*
- Confidentiality: *XML Encryption*
- Authentication and authorization: *SAML*
- Identity provisioning: *SPML*
- Managing access control policies: *XACML*

SAML



Linking ticket purchases to car rental



Assertions about authentication, attributes

The language of the PEP and PDP

This is about FEDERATION!!

Issuer ID and issuance timestamp

Assertion ID

Subject

Name and security domain

Subject's authentication data (optional)

Advice (optional additional information provided by the issuing authority)

Conditions under which the assertion is valid

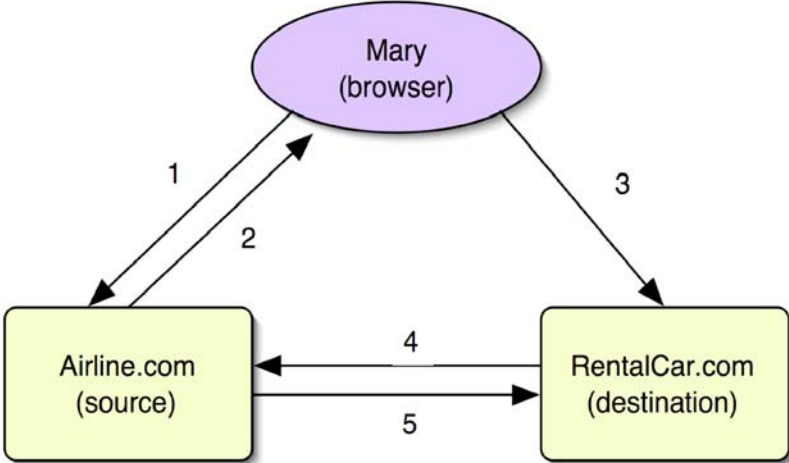
Assertion validity period (e.g. NotBefore and NotOnOrAfter)

Audience restrictions

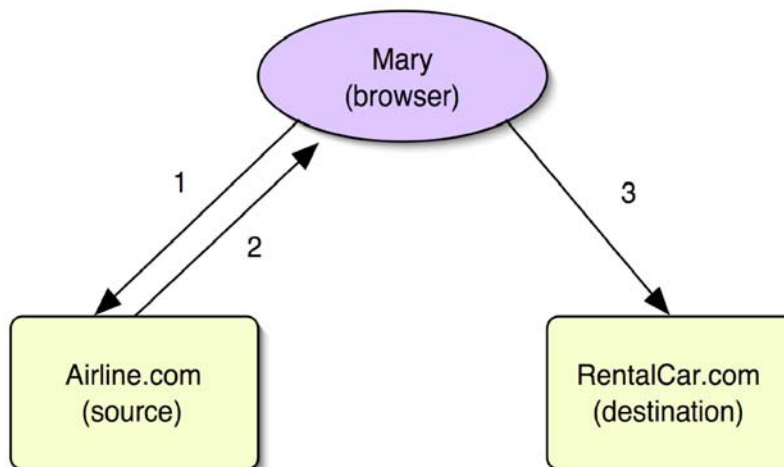
Target restrictions (intended URLs for the assertion)

Application specific conditions

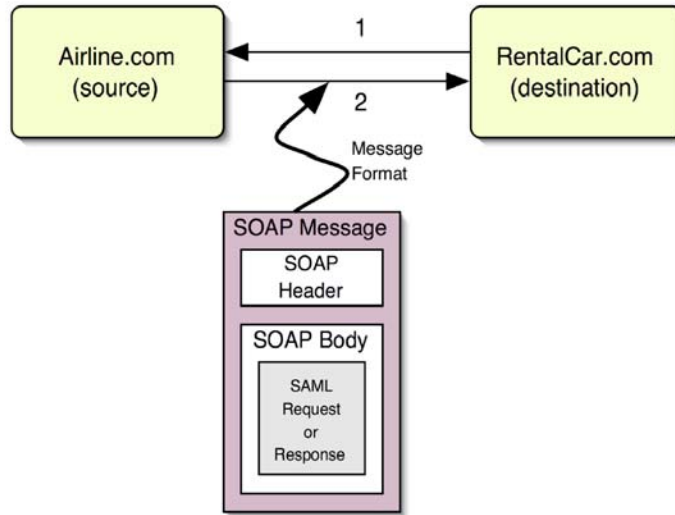
Browser Pull Use Case



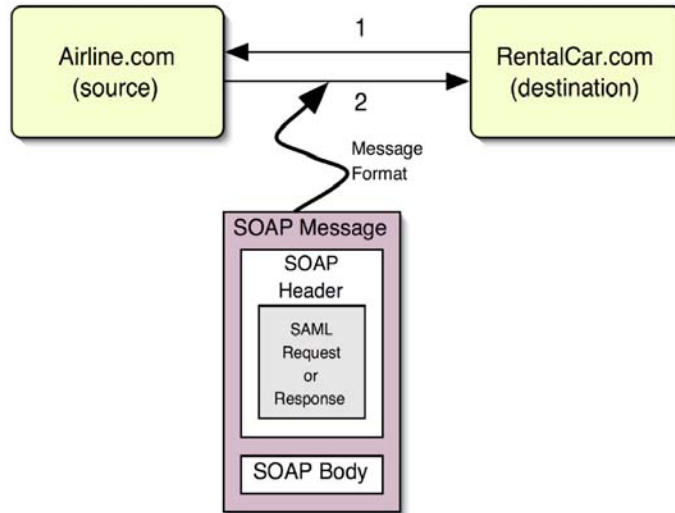
Browser Push Use Case



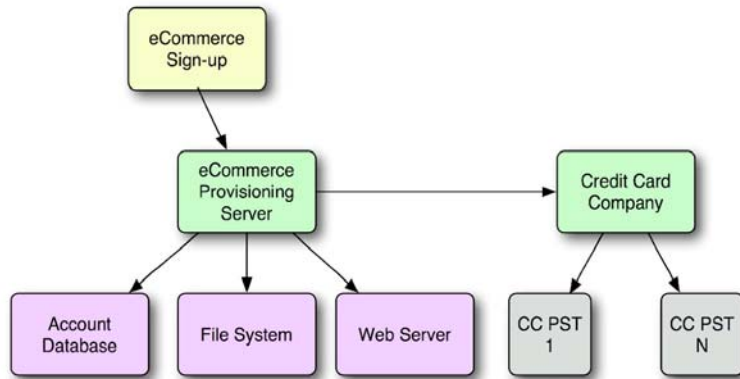
Direct Request Use Case

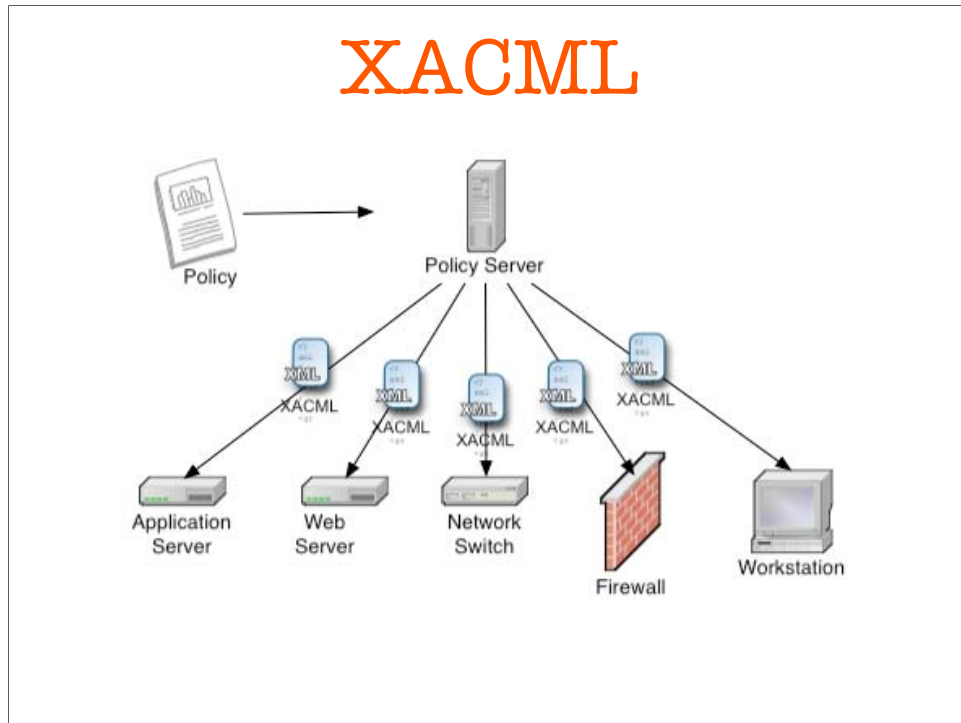


Web Service Use Case



SPML Example





Policies, and getting them to the right place at the right time.

eXtensible Access Control Mark-up Language

XML standards for storing, sharing, representing, and processing access control policies

Language of the Policy Decision Point (PDP)

SAML is about credentials

XACML is about processing credentials

XACML is more than a data standard

XACML is a programming language of sorts

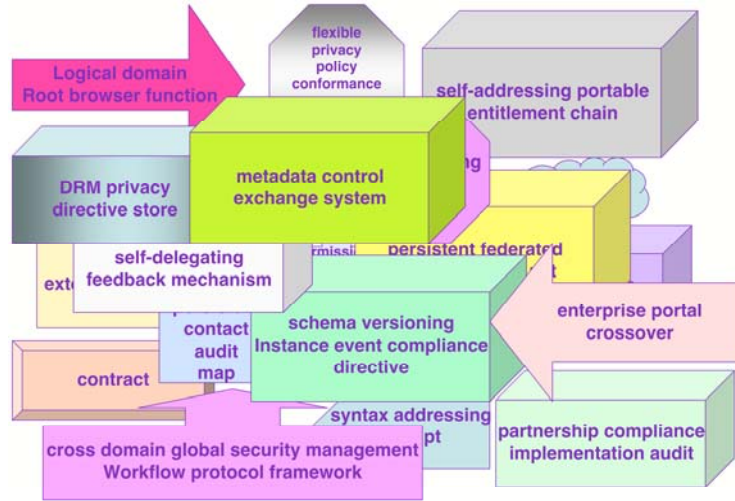
Rules can be based on

- Subject attributes
- Action to be taken
- Time of day
- Authentication mechanism
- Transport protocol
- Connectors

SourceID

- Open source project to implement Liberty Alliance specifications
- Available for Java and .NET
- Roadmap calls to support
 - SPML
 - XACML
 - FOAF
 - Shibboleth

Identity Infrastructure (as built)



Architecture courtesy of Doc Searls

Identity Management Architectures



City Planning

- Standardization
- Certification
- Management
 - Rules
 - Regulation
 - Enforcement

www.windley.com

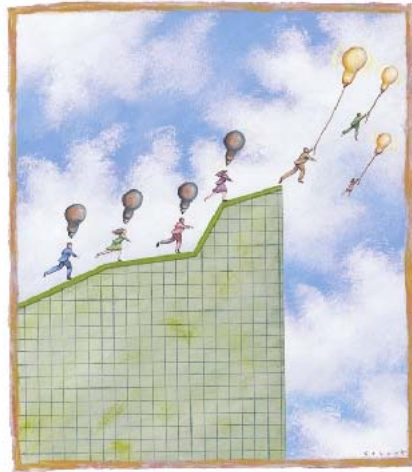
25

IMAs are like city planning. They provide context for other system activities and ensure interoperability.

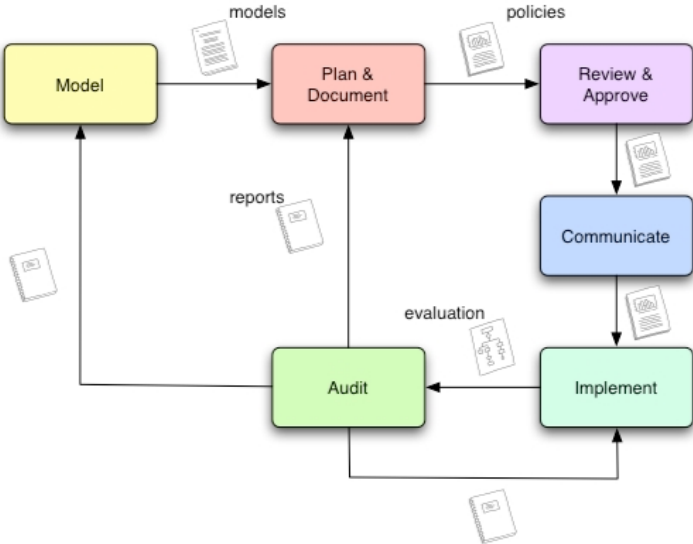
Creating a IMA Strategy

Key Steps

1. Governance
2. Business context
3. Resources
4. Policy
5. Interoperability framework
6. Reference architecture

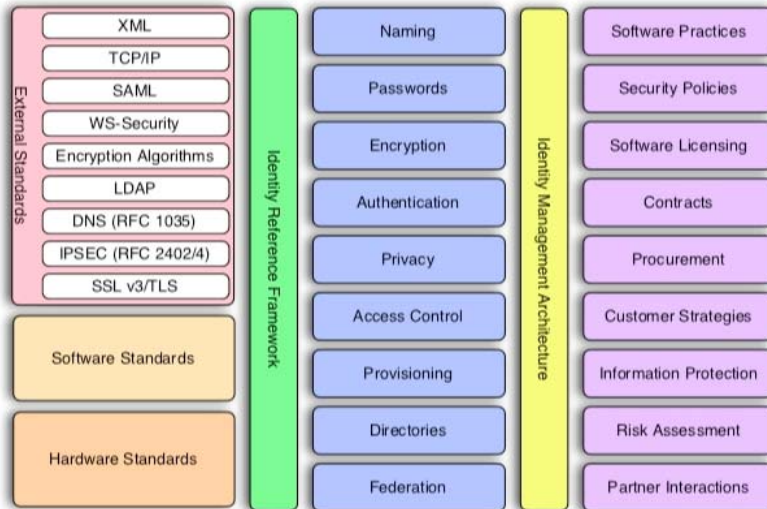


IMA Lifecycle



Governance formalizes this lifecycle

Identity Policy Stack



www.windley.com

28

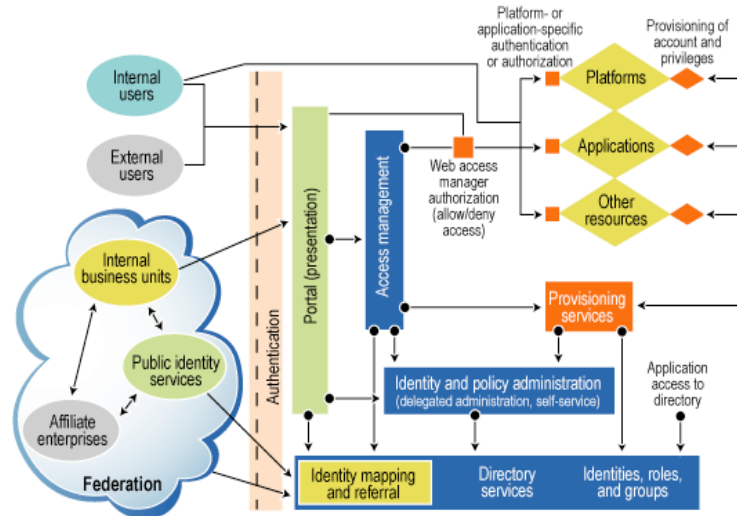
Many geeks don't like policies. We have an anarchist bent. Good policies create freedom.

The problem with most policies is they're ad hoc and reactionary

Policies provide a framework for building interoperability

Talk about stack.

IDMa Reference Architecture



Courtesy of The Burton Group

The End



- Business drivers
 - Service economy
 - Partner relationships
- Federation is more than technology
 - Governance
 - Politics
 - Legal
- IMAs provide context
 - Policy framework
 - Interoperability framework

www.windley.com

30

My book is about building IMAs

Contact Information

Contact me

- phil@windley.com
- www.windley.com
- www.eclab.byu.edu

Buy the book...

Get the paper...

Questions?



